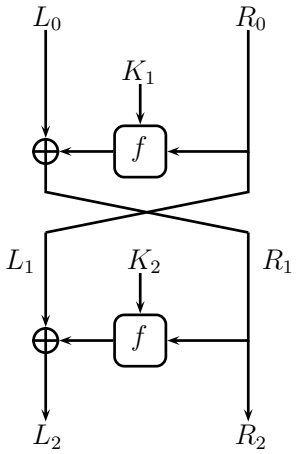
TD 4 : Chiffrements par bloc - Schémas de Feistel

Christina Boura

Exercice 1 *Feistel : Chiffrement et déchiffrement*
Montrer qu'en inversant l'ordre d'utilisation des sous-clés de tour dans un réseau de Feistel, on peut utiliser le même algorithme pour déchiffrer que celui utilisé pour chiffrer. On se limitera à un réseau de Feistel à 3 tours.

Exercice 2 *Réseau de Feistel*
Le réseau de Feistel de la figure suivante travaille sur un état de 8 bits :



La fonction f prend en entrée une sous-clé de 4 bits K_{i+1} et une donnée de 4 bits R_i, additionne bit-à-bit les deux entrées et applique au résultat une couche de confusion et ensuite une couche de diffusion :

$$\begin{aligned} f : \{0,1\}^4 \times \{0,1\}^4 &\rightarrow \{0,1\}^4 \\ f(K_{i+1}, R_i) &= P(S(K_{i+1} \oplus R_i)). \end{aligned}$$

où S est une boîte-S donnée par la table suivante :

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S(x)	8	6	7	9	3	12	10	15	13	1	14	4	0	11	5	2

et $P : \{0,1\}^4 \rightarrow \{0,1\}^4$ une permutation bit-à-bit donnée par

$$P = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \end{pmatrix}.$$

1. Chiffrer le message $m = 163_{10} = 1010\,0011_2$ avec les sous-clés $K_1 = 7$ est $K_2 = 12$. On notera le chiffré $c = (L_2|R_2)$. On considère que les bits de poids faible sont à droite.
2. Faire un dessin de l'algorithme de déchiffrement. Expliquer son fonctionnement. Est-il nécessaire que la fonction f soit inversible ?

Exercice 3 *Faiblesse des schémas de Feistel à 1 et 2 tours*

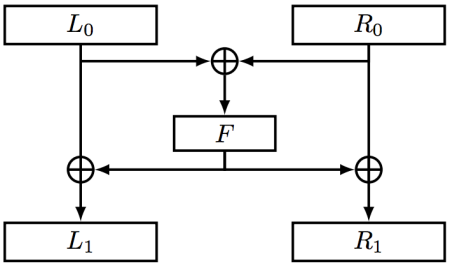
Un *distingueur* est un algorithme qui cherche, via un jeu de questions/réponses à distinguer un système de chiffrement donné E d'une permutation aléatoire. Un bon chiffrement par bloc ne doit pas pouvoir

être distingué d'une permutation aléatoire avec un nombre de requêtes relativement faible. Trouver un distingueur pour un chiffrement concret, revient à trouver une relation entre les entrées et les sorties du chiffrement qui est vérifiée avec une probabilité beaucoup plus élevée que pour une permutation aléatoire.

1. Décrire une façon de distinguer un schéma de Feistel à un tour d'une permutation aléatoire en utilisant une attaque à **clairs connus**.
2. Décrire une façon de distinguer un schéma de Feistel à deux tours d'une permutation aléatoire en utilisant une attaque à **clairs choisis**.

Exercice 4 *IDEA*
IDEA (*International Data Encryption Algorithm*) est un chiffrement symétrique par bloc, originellement présenté en 1990. Il emploie des clés de 128 bits pour chiffrer des bloc de 64 bits.

Le schéma IDEA est basé sur une variante du mécanisme de Feistel, dont la fonction de tour (on ignore ici l'addition des sous-clés) est décrite ci-dessous :



1. On se concentre pour l'instant sur la fonction de chiffrement n'ayant qu'un tour. Écrire les équations donnant l'expression du chiffré (L_1, R_1) en fonction du clair (L_0, R_0).
2. Montrer que ce schéma (on ne considère toujours qu'un tour) est inversible quelle que soit la fonction F et donner les formules décrivant le déchiffrement.
3. Décrire un schéma de Feistel à trois tours (sans la permutation finale des deux bloc L_3 et R_3) qui lui est équivalent.
4. Montrer comment distinguer la fonction de chiffrement $(L_0, R_0) \mapsto (L_1, R_1)$ d'une transformation aléatoire.
5. Même question si l'on empile plusieurs tours de chiffrement (par exemple, si on considère la fonction $(L_0, R_0) \mapsto (L_2, R_2)$ avec la même fonction F.

Exercice 5 *La non-linéarité est nécessaire*
Considérons un système de chiffrement par bloc qui suit le schéma de Feistel et dont la fonction f utilisée à chaque tour est constituée d'une transformation linéaire A, suivie d'une addition bit à bit avec la clé k, puis d'une seconde transformation linéaire B

$$f(x) = B(A(x) \oplus k).$$

Montrer comment il est possible d'attaquer un tel système.